UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/483,186	01/14/2000	Francisco Corella	10001559-1	8070

22879 7590 07/28/2005

HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER	
BROWN, CHRISTOPHER J	
ART UNIT	**PAPER NUMBER**
2134	

DATE MAILED: 07/28/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/483,186	CORELLA, FRANCISCO	
	Examiner	Art Unit	
	Christopher J. Brown	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 July 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 11/19/04, 6/24/05, 2/17/05
4) ☒ Interview Summary (PTO-413) Paper No(s)/Mail Date. *7/13/05*.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

The examiner makes note that an interview was held with the applicant on 7/13/2005. An interview summary is attached. The examiner did not receive the "official" version of the proposed amendment by 7/20/05 and had to proceed with the office action based on the response from the applicant filed 11/19/04.

Applicant's argument regarding 102 (Applicant's arguments, see filed 11/19/04, with respect to the rejection(s)of claim(s) 1, 2, 6, 7, 8, 13, 14, 18, 19, and 20 under 102(e) have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of is made.

Claim Rejections - 35 USC § 112

1. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1-24 are rejected, The meaning of every term used in any of the claims should be apparent from the descriptive portion of the specification with clear disclosure as to its import; and in mechanical cases, it should be identified in the descriptive portion of the

specification by reference to the drawing, designating the part or parts therein to which the term applies. A term used in the claims may be given a special meaning in the description. No term may be given a meaning repugnant to the usual meaning of the term. See MPEP 608.01 (o).

As per claims 1-24, the terms "Certificate Authority" and "certificate" by definition, include a digital signature. See Schneier page 185 "Public-key Certificates", Menezes page 548 "certification authority".

The applicant has used both terms in conjunction with "unsigned certificate". This is opposite of the common use of "Certificate Authority" and "certificate". Applicant must distinguish his invention from a Certificate Authority and a certificate.

The previous action as stated below, stands on the merits, as no Certificate Authority may issue unsigned certificates.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1,2,6,7,8,13,14,18,19, and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Andrews US 6,324645 in view of Fischer US 5,475,826.

3. **Claims 1, 2, 6, 7, 8, 13, 14, 18, 19, and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Andrews US 6,324,645 in view of Fischer US 5,475,826**

As per claims 1 and 13, Andrews discloses that a certificate authority issues a certificate to a user that binds the public key of the user to the users long term identification information, (Col 3 lines 26-30, 55-58). Andrews discloses that the subject demonstrates said subject has knowledge of a private key corresponding to the public key in the certificate, (Col 10 lines 34-37). Andrews does not teach a verifier maintaining cryptographic hashes.

Fischer teaches a system that has a verifier that maintains hashes of files in a security database. Fischer teaches that when files are presented they are scanned and a new hash is computed to verify the file matches the hash stored in the database, (Col 12 line 63-Col 13 line 5).

It would have been obvious to one of ordinary skill in the art to modify the certificate system of Andrews with the hash verifier of Fischer because the hash table verification would enhance the security of the system.

As per claims 2 and 14, Andrews discloses that the certificate has a date and time, (Validity) (Col 9 line 26, 34-36).

As per claims 6 and 18, Andrews discloses that the hash computed is a collision free hash, (Col 5 lines 30-34).

As per claims 7 and 19, Andrews discloses that the hash is a SHA hash (Col 5 line 34).

As per claims 8 and 20, Andrews discloses that the hash is an MD5 hash (Col 5 line 34).

Claim Rejections - 35 USC § 103

4. **Claims 3, 4 and 15, 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Andrews US 6,324,645 in view of Maruyama US 6,393,563**

As per claims 3 and 15, Andrews discloses that the certificate may not have a time and date, (Col 6 line 28).

As per claims 4 and 16, Andrews discloses a private key. Andrews does not disclose storing the private key on a smart card.

Maruyama disclose a private key may be stored on a smartcard, (Col 1 line 20, 53-56).

It would be obvious to modify the Andrews private key with Maruyama's smart card, because the smart card increases the security of key storage.

5. **Claims 5 and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Andrews US 6,324,645 in view of Kausik US 6,263,446.**

As per claims 5 and 17, Andrews does not disclose a software wallet.

Kausik discloses storing a private key in a software wallet, (Col 4 lines1-6).

It would be obvious to modify Andrews private key with Kausik's software wallet because the wallet increases the security of key storage.

6. **Claims 9 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Andrews US 6,324,645 in view of Gasser US 5,224,163.**

As per claims 9 and 21, Andrews does not disclose that the certificate is revoked based on the validity of the long term information and public key.

Gasser discloses that if the key of the certificate is compromised, it is revoked, (Col 7 lines 5-9).

It would be obvious to one skilled in the art to modify Andrews certificate revocation with Gassers invalid key revocation, because a subject that used an invalid key would not be accepted.

7. Claims 10, 11 and 22, and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Andrews US 6,324,645 in view of Micali US 5,793,868 in view of Boyle 6,212,636.

As per claims 10 and 22, Andrews does not disclose a revocation system involving hashes. Micali discloses a certificate revocation system where the certificate authority takes a hash of the certificates to be revoked, (Col 3 lines 18-23).

It would be obvious to one skilled in the art to modify Andrews revocation system with Micali's hashes, because hash's take less memory to store, and are well known for authentication properties in the art.

Boyle discloses that upon being notified that a certificate is revoked, that any data related to the certificate is erased from memory, (Col 21 line 59- 67).

It would be obvious to modify the Andrews Micali combination above with Boyle's method of deletion, because a subject would not want to accidentally use a revoked certificate.

As per claims 11 and 23, Andrews discloses that the certificate authority may mark the certificate as being invalid (CRL), (Col 6 lines 31-35).

8. Claims 12, and 24, are rejected under 35 U.S.C. 103(a) as being unpatentable over Andrews US 6,324,645 in view of Micali US 5,793,868 in view of Boyle 6,212,636 in view of Gasser US 5,224,163.

As per claims 12 and 24, Andrews's combination does not disclose deleting the certificate from the database once it has been revoked.

Gasser discloses a certificate authority (GNS) deletes the revoked certificate, (Col 7 lines 5-10).

It would be obvious to one skilled in the art to modify the Andrew's combination with Gasser's deletion method because the certificates are no longer useful.

Conclusion

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher J. Brown whose telephone number is (571)272-3833. The examiner can normally be reached on 8:30-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (571)272-3838. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Christopher J. Brown

David Y. Jung
Primary Examiner
7/28/05